АВТОМАТОВ ДЛЯ ГЕНЕРИРОВАНИЯ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Д. Е. Храбров

Учреждение образования «Гомельский государственный технический университет имени П. О. Сухого», Беларусь

Научный руководитель И. А. Мурашко

Важнейшим элементом встроенного самотестирования (англ. Built-in Self-test, BIST) является генератор псевдослучайных тестовых воздействий [1]. Самым используемым методом генерации тестовых воздействий максимальной длины является регистр сдвига с линейной обратной связью (англ. Linear feedback shift register, LFSR). Основным достоинством LFSR является его изученность и простота аппаратной реализации, для которой требуется лишь регистр сдвига и многовходовой сумматор по модулю два [2]. Однако использование LFSR не всегда оправдано для схем встроенного самотестирования ввиду сильной корреляции между последовательностями, формируемыми на различных разрядах генератора. Поэтому в последнее время внимание ученых направлено на использование альтернативных методов генерации псевдослучайных последовательностей максимальной длины, также называемых М-последовательностями. В частности, в качестве генераторов М-последовательностей рассматриваются генераторы на клеточных автоматах (КА) [3], [4].

Наиболее полно исследованы клеточные автоматы на основании правил 90 и 150 с нулевыми граничными условиями [5]. Для них созданы таблицы конфигураций, позволяющих формировать М-последовательности [6].

В общем случае клеточный автомат может быть рассмотрен как простая модель пространственно протяженного устройства, состоящего из ряда ячеек. Связи между

ячейками ограничены локальным взаимодействием. Если на крайние ячейки автомата постоянно подается логический ноль, то такие граничные условия называются нулевыми. Если в автомате последняя ячейка связана с первой и наоборот, то такие граничные условия называются циклическими.

В данной работе использован набор правил: 0, 170, 204, 102, 240, 90, 60, 150. Эти восемь правил представляют из себя все вариации одной клетки и двух соседей при использовании только сумматоров по модулю два. Отдельное место в этом наборе занимают правила 0 и 204, так как по сути сводят циклический клеточный автомат к автомату с нулевыми граничными условиями, но меньшей размерности (рис. 1).

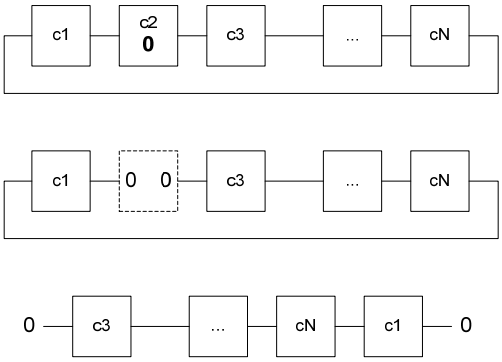

Рис. 1. Использование правила 0 в клеточном автомате с циклическими граничными условиями

В данной работе исследуется проблема классификации наборов правил КА, на которых генератор сможет выдавать последовательность максимальной длины. По рис. 1 видно, что при использовании правила 0 клеточный автомат фактически будет уменьшен на степень (то есть иметь размерность n–1), соответственно такой автомат не сможет генерировать последовательность длины 2^n-1, только $2^{n-1}-1$. Аналогичные результаты получаются для правила 204, которое формирует единичные граничные условия. Как следствие, для рассмотрения остались шесть правил: 170, 102, 240, 90, 60, 150.

При построении генератора на клеточных автоматах могут быть использованы различные комбинации правил, однако далеко не все полученные генераторы смогут выдавать последовательность максимальной длины. В таблице собраны сведения о не инвертированных наборах правил, генераторы на которых могут выдавать последовательность максимальной длины.

Выбор набора правил

Набор	**E**	**Ошибка в**	**I**	**P**	$\mathbf{A_{sp}}$	$\mathbf{A_{min}}$	$\mathbf{A_{max}}$	$\mathbf{L_{min}}$	$\mathbf{L_{max}}$	$\mathbf{L_{avg}}$
60,150	6	4,6,8,10,12,14	12	12	1,5	1,13	1,8	0,3	0,85	0,57
90,240	6	4,6,8,10,12,14	12	12	0,5	0,13	0,86			
60,240	4	8,12,13,14	11	11	0,5	0,06	0,93			
60,90,240	0	–	6	10	0,6	0,21	0,92			
60,90,150	0	–	6	10	1,3	1,07	1,76			
60,150,240	0	–	9	9	1	0,3	1,61			
90,150,240	0	–	6	8	1	0,23	1,61			
60,90,150,240	0	–	0	0	1	0,38	1,61			

Исследования показали, что примитивные полиномы конкретной степени существуют не для всех пар правил. Например, столбец «E» отвечает за ошибку (Error) – т. е. если для определенной степени не было найдено ни одного вектора правил на данном наборе и дающего M-последовательность, то такое состояние называется ошибкой. «Ошибка в» показывает, для каких именно степеней нет векторов на данном наборе правил. Столбец «I» – количество не пройденных тестов на неприводимость (Irreducibility). Тест на неприводимость считается не пройденным, если были найдены не все неприводимые характеристические полиномы для данной степени. «P» – количество проваленных тестов на примитивность (Primitiveness). Все примитивные полиномы неприводимы, обратное неверно. Однако тест на неприводимость имеет гораздо меньшую сложность, чем тест на примитивность. Поэтому сначала используется достаточно быстрый тест на неприводимость и в случае его прохождения выполняется тест на примитивность. Столбец «A_{sp}» отвечает за удельные аппаратные затраты, считая что правила в наборе равновероятны. Известно, что аппаратная реализация генераторов на клеточных автоматах выполняется с использованием только триггеров и сумматоров по модулю два. Например, значение «0,5» в столбце «A_{sp}» означает, что удельные аппаратные затраты для данного набора равны пол сумматора по модулю два на разряд. В столбцах «A_{min}» и «A_{max}» приведены минимальные и максимальные аппаратные затраты для генератора на различных конфигурациях правил. Также для аналогии рассмотрим все LFSR тринадцатой степени, генерирующие последовательность максимальной длины. Пример порождающего полинома с минимальными аппаратными затратами для LFSR: $x^{13} + x^4 + x^3 + x + 1$. Аппаратные затраты в этом случае составляют один пятивходовой сумматор по модулю два, который можно представить как 4 двухвходовых сумматора, т. е. $LFSR_{min} = L_{min} = 4/13 = 0{,}3$. В наихудшем с точки зрения аппаратных затрат полиноме содержится 12 членов, т. е. аппаратные затраты составляют 11 двухвходовых сумматоров по модулю два: $LFSR_{max} = 11/13 = 0{,}85$. Можно предположить, что в среднем аппаратные затраты будут равны: $LFSR_{avg} = (LFSR_{max} + LFSR_{min})/2 = 0{,}58$.

Методика выбора конкретного набора правил для генератора в зависимости от критерия приведена на рис. 2.

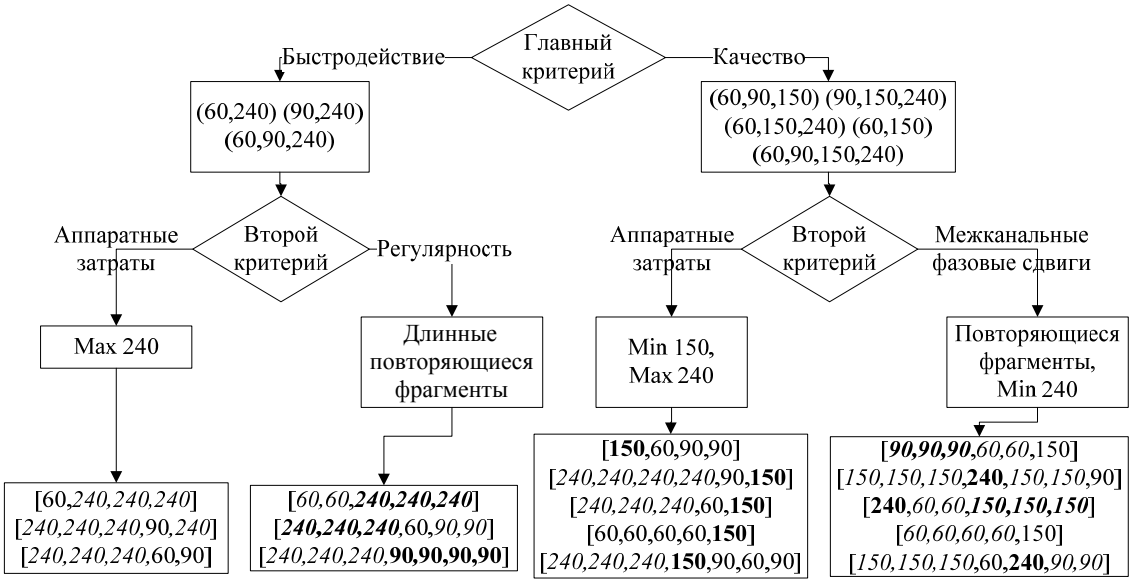

Рис. 2. Схема выбора набора правил

Минимальная реализация может быть выполнена на правилах 240 (0 сумматоров), 60 и 90 (по одному сумматору). Соответственно, генератор на этих правилах содержит максимум один сумматор по модулю два на разряд. В то же время если используется большое количество ячеек с правилом 240, то аппаратные затраты снижаются (см. таблицу). Однако их недостаток заключается в том, что в данном случае фрагменты генератора повторяют работу LFSR. Чтобы улучшить качество, мы можем использовать конфигурации, содержащие правила 60 и 90.

С другой стороны, если главным критерием является качество, то тогда необходимо минимизировать число ячеек с правилом 240 (межканальный сдвиг для этого разряда равен единице). Заметим, что расчет фазовых сдвигов упрощается при регулярной структуре генераторов, т. е. наличии фрагментов с одинаковыми правилами функционирования. Соответственно, можно выбирать конфигурации, включающие правила и 150, и 60, и 240 – можно набирать любую доступную конфигурацию, при этом минимизируя количество ячеек с правилом 240.

В работе исследована проблема проектирования генераторов псевдослучайных тестовых наборов на клеточных автоматах с расширенным набором правил – 0, 170, 204, 102, 240, 90, 60, 150. Рассмотрена проблема выбора наилучшего поднабора из приведенных правил. Выяснено, что генераторы далеко не на всех выборках способны генерировать последовательность максимальной длины. Предложен метод выбора наилучшего набора правил для каждой конкретной ситуации.

Литература

1. Agrawal V., Bushnell M. Essentials of Electronic Testing for Digital, Memory, and Mixed-Signal VLSI Circuits. Springer, 2000. – P. 712.
2. Golomb, S. W. Shift register sequences / S. W. Golomb // San Francisco: Holden-Day, 1967. – P. 224.
3. Hortensius, P. D. Parallel random number generation for VLSI systems using cellular automata / P. D. Hortensius // IEEE Transactions on Computers. – 1989. – Vol. 38 (10). – P. 1466–1473.
4. del Reya, A. M. Reversibility of linear cellular automata / A. M. del Reya, G. R. Sanchez // Applied Mathematics and Computation. – 2011. – Vol. 217. – P. 8360–8366.
5. Ярмолик, В. Н. Реализация генератора псевдослучайной последовательности на клеточных автоматах / В. Н. Ярмолик, И. А. Мурашко // Автоматика и вычислительная техника. – 1993. – № 3. – С. 9–13.
6. Cattell, K. Minimal cost one-dimensional linear hybrid cellular automata of degree through 500 / K. Cattell, S. Zhang // Journal of Electronic Testing: Theory and Applications. – 1995. – Vol. 6. – P. 255–258.